Method And System For User Authentication

FIELD OF INVENTION

The present invention relates broadly to a method and system for user authentication.

BACKGROUND

Computer accessible application programs are susceptible to unauthorized access. Typically, the login interface of such programs comprises just one level of security. The verification of one user name and one password is typically sufficient to gain access to the program. For example a simple phishing incident is all it takes to compromise thousands of e-business user credentials. After stealing the user names and passwords, an authorised user can freely access the users' online account with ease. For example, this puts at risk many existing E-business systems for automating sales force information processing, customer relationship management, financial management, supply chain management and e-commerce.

SUMMARY

In accordance with a first aspect of the present invention there is provided a method for user authentication during a log-in session on a first device, the method comprising generating and displaying on the first device an image associated with a current log-in session of the user; capturing the image utilising a second device; sending both image data corresponding to the captured image and Identification (ID) data associated with the second device from the second device to the first device; and granting access to the first device based on matching the image data received with the generated image and matching the ID data received against an ID data database.

The image associated with the current log-in session may, at least in part, be randomly generated.

The image may comprise a first section containing a visual guide for identifying a location of the image in the captured image; and a second section containing data associated with the current log-in session.

The second section associated with the current log-in session may, at least in part, be randomly generated.

The visual guide may comprise a regular geometric shape with a central dot.

The regular geometric shape may be one of a group consisting of a circle; a triangle; and a square, the dot being concentric with the circle, the triangle, or the square respectively.

The ID data associated with the second device may comprise data inherently incorporated in a data communication between the second and first devices.

The ID data may comprise one or more of a group consisting of Mobile Station ISDN Number (MSISDN); International Mobile Equipment Identity (IMEI) number; International Mobile Subscriber Identity (IMSI); Mobile Identification Number (MIN); and System Identification Code (SID).

The log-in session may comprise a graphical user interface comprising a username field for entering user name; a password field for entering password; and an area for displaying the image associated with the current log-in session of the user;

The first device may comprise one or more of a group consisting of a personal computer; and an automated teller machine;

The second device may comprise one or more of a group consisting of a Personal Digital Assistant; a digital camera; and a mobile phone.

Sending both the image data corresponding to the captured image and the ID data associated with the second device from the second device to the first device may be through a wireless connection.

Sending both the image data corresponding to the captured image and the ID data associated with the second device from the second device to the first device may be through a wired connection.

Both the image data corresponding to the captured image and the ID data may be saved by the second device into a memory card, and the first device may receive both the image data corresponding to the captured image and the ID data from the memory card.

The wireless connection may comprise one or more of a group consisting of Bluetooth; Infrared; Wireless LAN; Ultra-Wideband Radio (UWB); and HomeRF.

The wired connection may comprise one or more of a group consisting of USB ports and cables; Firewire ports and cables; Universal Asynchronous Receiver-Transmitter (UART) based Serial ports and cables; and parallel ports and cables.

The memory card may be one of a group consisting of MultiMedia Card (MMC); Secure Digital (SD) cards; Compact Flash (CF) cards; Mini Secure Digital card (Mini SD); Reduced-Size MultiMediaCard (RSMMC); Memory Stick (MS); Memory Stick Duo (MS Duo); Memory Stick Pro (MS Pro); Memory Stick Duo Pro (MS Duo Pro); and High Speed Memory Stick (HS MS).

In accordance with a second aspect of the present invention there is provided a system for user authentication during a log-in session comprising an ID data database; means for generating an image associated with a current log-in session of the user; means for displaying the image associated with a current log-in session of the user; means for receiving both image data corresponding to a captured image of the displayed image and Identification (ID) data associated with an external device utilised to capture the image data; and means for granting access

to the system based on matching the image data received with the generated image and matching the ID data received against the ID data database.

The image associated with the current log-in session may, at least in part, be randomly generated.

The image may comprise a first section containing a visual guide for identifying a location of the image in the captured image; and a second section containing data associated with the current log-in session.

The second section associated with the current log-in session may, at least in part, be randomly generated.

The visual guide may comprise a regular geometric shape with a central dot.

The regular geometric shape may be one of a group consisting of a circle; a triangle; and a square, the dot being concentric with the circle, the triangle, or the square respectively.

The ID data associated with the second device comprises data may be inherently incorporated in a data communication between the second and first devices.

The ID data may comprise one or more of a group consisting of Mobile Station ISDN Number (MSISDN); International Mobile Equipment Identity (IMEI) number; International Mobile Subscriber Identity (IMSI); Mobile Identification Number (MIN); and System Identification Code (SID).

The log-in session comprises a graphical user interface comprising a username field for entering user name; a password field for entering password; and a area for displaying on the first device the image associated with the current log-in session of the user.

The first device may comprise one or more of a group consisting of a personal computer; and an automated teller machine.

The second device may comprise one or more of a group consisting of a Personal Digital Assistant; a digital camera; and a mobile phone;

Sending both image data corresponding to the captured image and Identification (ID) data associated with the second device from the second device to the first device may be through a wireless connection.

Sending both image data corresponding to the captured image and the ID data associated with the second device from the second device to the first device may be through a wired connection.

Both the image data corresponding to the captured image and the ID data may be saved by the second device into a memory card, and the first device may receive both the image data corresponding to the captured image and the ID data from the memory card.

The wireless connection may comprise one or more of a group consisting of Bluetooth; Infrared; Wireless LAN; Ultra-Wideband Radio (UWB); and HomeRF.

The wired connection may comprise one or more of a group consisting of USB ports and cables; Firewire ports and cables; Universal Asynchronous Receiver-Transmitter (UART) based Serial ports and cables; and parallel ports and cables.

The memory card may be one of a group consisting of MultiMedia Card (MMC); Secure Digital (SD) cards; Compact Flash (CF) cards; Mini Secure Digital card (Mini SD); Reduced-Size MultiMediaCard (RSMMC); Memory Stick (MS); Memory Stick Duo (MS Duo); Memory Stick Pro (MS Pro); Memory Stick Duo Pro (MS Duo Pro); and High Speed Memory Stick (HS MS).

In accordance with a third aspect of the present invention there is provided a system for user authentication during a log-in session comprising an ID data database a graphics generator for generating an image associated with a current log-in session of the user; a screen for displaying the image associated with a current log-in session of the user; a transceiver for receiving both image data corresponding to a captured image of the displayed image and the ID data associated with an external device utilised to capture the image data; and an authentication unit for granting access to the system based on matching the image data received with the generated image and matching the ID data received against the ID data database.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will be better understood and readily apparent to one of ordinary skill in the art from the following written description, by way of example only and in conjunction with the drawings, in which:

Figure 1 is a schematic diagram illustrating a user authentication system according to an example embodiment of the present invention.

Figure 2 is a diagram illustrating a login dialog box according to the example embodiment of the present invention.

Figure 3 is a flowchart illustrating the operation of the user authentication system according to the example embodiment of the present invention.

Figure 4 is a diagram illustrating a tag image utilised in the example embodiment of the present invention.

Figure 5 is a schematic drawing illustrating a computer system for implementation of a user authentication method and system according to an example embodiment of the present invention.

Figure 6 shows a flowchart illustrating a method for user authentication during a log-in session on a first device in an example embodiment.

DETAILED DESCRIPTION

The example embodiment described provides a method and system for user authentication on a computer. During login, a tag image is randomly generated and displayed. Next, the user captures the tag image displayed on a monitor screen of the computer with his mobile phone camera. This is followed by the user sending the image from his mobile phone to the computer wirelessly. The user's unique subscriber information or specific mobile device information is sent to the computer as part of the wireless transmission. Next, the identity of the user is verified by matching his unique subscriber information or mobile device specific information with pre-stored information at the computer and by matching the camera captured tag image with the randomly generated tag image at the computer.

Figure 1 shows the system setup of an example embodiment of the present invention. The authentication system 100 comprises a computer 102, a Bluetooth enabled mobile phone 104 with camera function and a wireless personal computer (PC) card 114. The mobile phone 104 and wireless personal computer (PC) card 114 are connected through a wireless link 116 via Bluetooth Technology.

On one end, the computer 102 comprises a computer monitor 118 with a computer screen 106 displaying a graphical user interface (GUI) of a computer application program. The computer application program may be web-based or local PC based. The computer 102 maintains a database of registered user account details storing information such as the Subscriber Identification Module (SIM) card or mobile phone specific information of the user's mobile phone 104, the user account number and personal identification number (pin) number. Only registered users with one or more user accounts can access the application program. The GUI contains computer mouse cursor clickable, keyboard linked and/or computer keyboard hotkey enabled buttons, textboxes, password enabled textboxes etc for user interaction with the computer application program.

Figure 1 shows the GUI of the computer application program in the form of a login dialog box 110 displaying a generated Tag image 112 that is used in user authentication. This GUI is invoked at the start of the user login session of the computer application program. In the example embodiment, the user's mobile phone number, also known as the Mobile Station ISDN Number (MSISDN), is used for user authentication. It is appreciated that the International Mobile Equipment Identity (IMEI) number, International Mobile Subscriber Identity (IMSI), Mobile Identification Number (MIN), System Identification Code (SID) etc may also be used. SIM card or mobile phone specific information is used because the information is unique to the user's mobile phone or mobile telephone network subscription plan and therefore can be seen as unique to each individual user.

On the other end, the mobile phone 104 comprises a screen 108 displaying a GUI of a camera shooting application program, which shows the view captured by the mobile phone camera. In the example embodiment, the screen 108 is used to aid the user to adjust the mobile phone camera such that the Tag image 112 is fully captured. In the example embodiment, the wireless PC card 114 is Bluetooth enabled and is connected to the computer 102 via a Universal Serial Bus (USB) port. IThe connection between the wireless PC card 114 and the computer 102 may be made via USB ports, Firewire ports, Universal Asynchronous Receiver-Transmitter (UART) based Serial ports, Parallel ports etc. The mobile phone can be any mobile device with camera function and wireless technology for linking with the wireless PC card such as a Personal Digital Assistant (PDA), a digital camera etc.

Figure 2 shows an example display of the login dialog box 110. The dialog box 110 displays a normal textbox 202, a password enabled textbox 204, a login button 206, an exit button 208 and a Tag image 112.

Textbox 202 is for users of the application program to key in their account name. Textbox 204 is for users of the application program to key in their pin number. As a security measure, a single character "*" is displayed for every keyed in

character so as to prevent viewing of the pin. The exit button 208 is for users to click on to end the login session, which also exits the application program.

The login button 206 is for users to click on to cross a first level of security after the account name textbox 202 and password textbox 204 fields are completed and verified to be the correct account name and pin of the user. The verification involves matching the keyed in account name and pin of the user with the account name and pin of the user pre-stored in the database of registered user details maintained by the computer 102. The user account number and pin may be in alphanumeric or numeric format and may be set to be case sensitive.

The Tag image 112 is randomly generated and displayed in the login dialog box 110. The purpose of the Tag image 112 is for use in a second level of user authentication. The use of a randomised tag image helps to make it difficult for unauthorised users to pass off as the actual user. If the same image was used repeatedly during login, an unauthorised user who has acquired the image may gain illegal access. Details of the second level of user authentication are discussed below.

Figure 3 is a flowchart illustrating the authentication process in the example embodiment. At step 300, a user wanting to access an application program of the computer 102 that requires user authentication starts the application program. After executing the application program on the computer 102, a user login session is started and the login dialog box 110 is displayed on the computer screen 106. At the same time, the computer 102 randomly generates a Tag image 112 and displays it in the dialog box 110.

At step 302, the user keys in his details into the textboxes in the login dialog box 110. After filling the account number textbox 202 and pin textbox 204 with his account number and pin respectively, the user clicks on the login button 206.

If the account number and pin do not match, the user is prompted to key in his details again at step 302.

In step 304, a check is made to determine if the user details are correct. If the account number and pin match with the pre-stored account number and pin in the database of registered user details maintained by the computer respectively, a first level of security is considered cleared. If step 304 returns false, processing returns to step 302, otherwise, at step 306, the application program activates the computer 102 to scan data input from the wireless PC card 114. Next, at step 307, a check is made to determine if the captured image data is received.

To login, the user first captures the Tag image 112 using the built-in camera of his mobile phone 104. The screen 108 on the mobile phone 104 helps the user to view and adjust the camera such that the entire image 112 on the computer monitor 106 is captured in a picture snapshot. The captured image may be taken close up, or at a distance depending on the resolution of camera.

After capturing the full Tag image 112 as a picture, the user sends the picture 112 wirelessly via Bluetooth from his mobile phone 104 to the wireless PC card 114. Besides containing data of the captured picture, which contains the tag image 112, data packets that are sent wirelessly to the wireless PC card 114 contain data of the user mobile phone number without the need for the user to key in the number as a separate message or a message attached with the captured image.

In the example embodiment, a java program residing on the mobile phone 104 is operated to instruct the inclusion of the data of the user mobile phone number in the transmission to the wireless PC card 114. However, it will be appreciated that in different embodiments, this feature may be implemented in different ways. For example, an application residing on the computer 102 may poll the mobile phone 104 for obtaining the relevant data, or the transmission technique utilised between the mobile phone 104 and the computer 102 might be of a type in which the relevant data is inherently incorporated in the transmission.

After the picture 112 is sent wirelessly via Bluetooth from the user mobile phone 104 to the wireless PC card 114, the data of the captured image and the user mobile phone number will be received by the computer 102. Upon receipt by the

computer, the check performed at step 307 will return true, otherwise processing returns to step 306.

If step 307 returns true, the application program automatically executes an authentication routine to verify if the user is authorised to access the program at step 312.

At step 314 a check is made to determine if the mobile number matches the pre-stored mobile number. At the computer, the authentication routine verifies the user's identity by matching the received user mobile phone number with pre-stored information provided by the user during registration for a user account for the application program.

If there is no match in step 314, login is unsuccessful and the user is denied access at step 318. In this case, the login session may end and exit the application program or return to step 302 after erasing the account number and pin. A limited number of tries may be given before the program locks out the user account by disallowing any further attempts to access the program.

If the user mobile phone number received by the computer 102 matches the pre-stored user mobile phone number, a second level of security is considered cleared. Next, at step 316 at the computer, the authentication routine matches the randomly generated Tag image 112 with the tag image captured in the received picture.

If the captured tag image matches the generated Tag image 112, a third level of security is considered cleared, login is successful and user access to the application program is granted at step 320. If there is no match, login is unsuccessful and the user is denied access at step 318. Similarly, in this case, the login session may end and exit the application program or return to step 302 after erasing the account number and pin. A limited number of tries may be given before the program locks out the user account by disallowing any further attempts to access the program.

Embodiments of the present invention may use the following tag image and adopt the following method to match the randomly generated Tag image 112 with the captured tag image in the received picture. The embodiment of the present invention is not limited to the tag image or the method of detecting and matching tag images as described below.

With reference to Figure 4, the Tag image 112 may be in a plurality of sections. There may be a first section 402 containing a circle 406 with a concentric dot 404 at its centre that define the location of the tag image 112 in a given area, even when the image is captured from a distance and the capturing may include a background, and a second section 408, which may contain data. The first section 402 is joined to second section 408 by a link 414. In the example embodiment, the background colour of the immediate area closest to and outlining the tag and filling the enclosed area within the tag is uniform and set as white. A uniform colour enables easy detection of the tag image within the captured picture.

The circle 406 with a concentric dot 404 is the easiest geometric figure for the computer 102 to locate in the captured tag image as the circle can be located from any angle. However, any other regular geometric shape such as, for example, an equilateral triangle, a square, regular pentagon, regular hexagon, regular heptagon, regular octagon, and so forth may be used. A regular shape is used as all sides are of equal length. This introduces consistencies, which can be easily followed by the image processor (in this case computer 102), when viewing the sides.

The randomly generated portion of the Tag image 112 in the second section 408 may be presented in the form of dots, boxes etc. In Figure 4, the second section 408 has a border 412 and dots 410 are contained within the border 412.

The arrangement, number, shape, size etc. of the dots may be changed in a random manner. Therefore, in the example embodiment, each randomly generated Tag image 112 corresponds to a unique presentation of the Tag image 112. The unique presentation is assigned to a current login.

In the example embodiment, upon receiving the captured tag image, the computer locates the first section 402 containing a circle 406 with a concentric dot 404 at its

centre, which defines the location of the tag image 112 in a given area. After the first section 402 is detected in the captured tag image, a search around the perimeter of circle 406 finds link 414, which leads to the border 412, and within the border 412, the computer 102 detects the data presented in the form of the dots 410. After locating the data 410 , the computer then matches the captured tag image with the current displayed Tag image 112 in the database maintained by the computer 102. The result of the matching determines whether user access is allowed.

In another example embodiment, the computer is a remote automated teller machine (ATM). The ATM has a Bluetooth interface incorporated as part of its system. The ATM may have access to a server database or maintain its own database of bank user accounts.

In this embodiment, the user wishes to login to his bank account at the ATM. Upon indicating his intention to perform bank transactions, for example, by slotting his ATM card into the card reader of the ATM, a user authentication GUI such as the login dialog box in Figure 2 is displayed on the monitor of the ATM. The login dialog box contains fields for entering the account name and account password, and a randomly generated tag image. To login, the user keys in the correct account name and account password followed by clicking a login button on the ATM user interface to clear a first level of security.

Next, the user captures fully the randomly generated tag image displayed in the login dialog box in a picture using his mobile phone camera. Then, utilising his Bluetooth enabled mobile phone, the user sends the picture containing the captured Tag image wirelessly to the ATM via Bluetooth.

At the ATM, the ATM performs user authentication by using the MSISDN of user's SIM card, which is sent with the picture without the user actually inputing the number into his mobile phone. Next, matching is performed between the MSISDN of the user's mobile phone and the user's pre-stored MSISDN in the server database accessible by the ATM. If the MSISDN matches, a second level of security is cleared.

Next, the ATM compares the received picture with the randomly generated tag image. The tag image and method of detecting and matching tag images used in this example embodiment may be as described above. If there is a match in the generated and captured images, the login is successful. Otherwise, the login is unsuccessful and the user is denied access.

The method and system of the example embodiments can be implemented on a computer system 500, schematically shown in Figure 5. It may be implemented as software, such as a computer program being executed within the computer system 500, and instructing the computer system 500 to conduct the method of the example embodiment.

The computer system 500 comprises a computer module 502, input modules such as a keyboard 504 and mouse 506 and a plurality of output devices such as a display 508, and printer 510.

The computer module 502 is connected to a computer network 512 via a suitable transceiver device 514, to enable access to e.g. the Internet or other network systems such as Local Area Network (LAN) or Wide Area Network (WAN).

The computer module 502 in the example includes a processor 518, a Random Access Memory (RAM) 520 and a Read Only Memory (ROM) 522. The computer module 502 also includes a number of Input/Output (I/O) interfaces, for example I/O interface 524 to the display 508, and I/O interface 526 to the keyboard 504.

The components of the computer module 502 typically communicate via an interconnected bus 528 and in a manner known to the person skilled in the relevant art.

The application program is typically supplied to the user of the computer system 500 encoded on a data storage medium such as a CD-ROM or floppy disk and read utilising a corresponding data storage medium drive of a data storage device 530. The application program is read and controlled in its execution by

the processor 518. Intermediate storage of program data maybe accomplished using RAM 520.

Figure 6 shows a flowchart illustrating a method for user authentication during a log-in session on a first device in an example embodiment. At step 600 an image associated with a current log-in session of the user is generated and displayed on the first device. At step 602, the image is captured utilising a second device. At step 604, both image data corresponding to the captured image and Identification (ID) data associated with the second device are sent from the second device to the first device. At step 606, access to the first device is granted based on matching the image data received with the generated image and matching the ID data received against an ID data database.

It will be appreciated by a person skilled in the art that numerous variations and/or modifications may be made to the present invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects to be illustrative and not restrictive.

For example, it is appreciated that the wireless technology linking the computer and the mobile device can be Bluetooth, Infrared, Wireless LAN, Ultra-Wideband Radio (UWB), HomeRF etc.
Also, it is appreciated that embodiments of the present invention may transmit the data of the captured picture through a wired connection using e.g. USB ports and cables, Firewire ports and cables, Universal Asynchronous Receiver-Transmitter (UART) based Serial ports and cables, and parallel ports and cables etc.

It is further appreciated that aside from wireless and wired connections, the computer in the embodiments of the present invention may receive the data of the captured image from a digital media reader that is capable of retrieving data from memory cards/sticks such as MultiMedia Card (MMC), Secure Digital (SD) cards, Compact Flash (CF) card, Mini Secure Digital card (Mini SD), Reduced-Size MultiMediaCard (RSMMC), Memory Stick (MS), Memory Stick Duo (MS Duo), Memory Stick Pro (MS Pro), Memory Stick Duo Pro (MS Duo Pro), High Speed Memory Stick (HS MS) etc.

Furthermore, it is appreciated that the embodiments of the present invention may be employed on personal computers, photocopier machines, fax machines etc in places where access control to data resources or use of machinery may be necessary such as in an office, a laboratory, a museum etc. Each user is required to clear the levels of security as described previously before access to the data resources or use of machinery is granted.

Extending the concept of access control, other examples utilising embodiments of the present invention are access control for a safe, a locker, a locked entrance/exit door etc. The computer in these exmbodiments may take the form of a microcontroller with accompanying firmware. A Liquid Crystal Display (LCD) monitor, Cathode Ray Tube (CRT) monitor or the like may be connected to the video Input/Output (I/O) port of the computer to display the user authentication GUI such as the login dialog box in Figure 2. A wireless or wired connection as described previously may be incorporated to the system architecture of the computer for receiving image data corresponding to the captured image and identification data associated with the user's camera enabled device. In order to gain access to open the safe, the locker, the locked entrance/exit door etc each user is required to clear the levels of security as described previously.

CLAIMS

1. A method for user authentication during a log-in session on a first device, the method comprising:

generating and displaying on the first device an image associated with a current log-in session of the user;

capturing the image utilising a second device;

sending both image data corresponding to the captured image and Identification (ID) data associated with the second device from the second device to the first device; and

granting access to the first device based on matching the image data received with the generated image and matching the ID data received against an ID data database.

2. The method as claimed in claim 1, wherein the image associated with the current log-in session is, at least in part, randomly generated.

3. The method as claimed in claims 1 or 2, wherein the image comprises:

a first section containing a visual guide for identifying a location of the image in the captured image; and

a second section containing data associated with the current log-in session.

4. The method as claimed in claim 3, wherein the second section associated with the current log-in session is, at least in part, randomly generated.

5. The method as claimed in claim 3, wherein the visual guide comprises a regular geometric shape with a central dot.

6. The method as claimed in claim 5, wherein the regular geometric shape is one of a group consisting of a circle; a triangle; and a square, the dot being concentric with the circle, the triangle, or the square respectively.

7. The method as claimed in any one of the preceding claims, wherein the ID data associated with the second device comprises data inherently incorporated in a data communication between the second and first devices.

8. The method as claimed in any one of the preceding claims, wherein the ID data comprises one or more of a group consisting of:

Mobile Station ISDN Number (MSISDN);

International Mobile Equipment Identity (IMEI) number;

International Mobile Subscriber Identity (IMSI);

Mobile Identification Number (MIN); and

System Identification Code (SID).

9. The method as claimed in any one of the preceding claims, wherein the log-in session comprises a graphical user interface comprising:

a username field for entering user name;

a password field for entering password; and

an area for displaying the image associated with the current log-in session of the user;

10. The method as claimed in any one of the preceding claims, wherein the first device comprises one or more of a group consisting of:

a personal computer; and

an automated teller machine;

11. The method as claimed in any one of the preceding claims, wherein the second device comprises one or more of a group consisting of:

a Personal Digital Assistant;

a digital camera; and

a mobile phone.

12. The method as claimed in any one of the preceding claims, wherein sending both the image data corresponding to the captured image and the ID data associated with the second device from the second device to the first device is through a wireless connection.

13. The method as claimed in any one claims 1 to 11, wherein sending both the image data corresponding to the captured image and the ID data associated with the second device from the second device to the first device is through a wired connection.

14. The method as claimed in any one of claims 1 to 12, wherein both the image data corresponding to the captured image and the ID data are saved by the second device into a memory card, and the first device receives both the image data corresponding to the captured image and the ID data from the memory card.

15. The method as claimed in claim 12, wherein the wireless connection comprises one or more of a group consisting of:

Bluetooth;
Infrared;
Wireless LAN;
Ultra-Wideband Radio (UWB); and
HomeRF.

16. The method as claimed in claim 13, wherein the wired connection comprises one or more of a group consisting of:

USB ports and cables;
Firewire ports and cables;
Universal Asynchronous Receiver-Transmitter (UART) based Serial ports and cables; and
parallel ports and cables.

17. The method as claimed in claim 14, wherein the memory card is one of a group consisting of:

MultiMedia Card (MMC);
Secure Digital (SD) cards;
Compact Flash (CF) cards;
Mini Secure Digital card (Mini SD);
Reduced-Size MultiMediaCard (RSMMC);

Memory Stick (MS);
Memory Stick Duo (MS Duo);
Memory Stick Pro (MS Pro);
Memory Stick Duo Pro (MS Duo Pro); and
High Speed Memory Stick (HS MS).

18. A system for user authentication during a log-in session comprising:

an ID data database;

means for generating an image associated with a current log-in session of the user;

means for displaying the image associated with a current log-in session of the user;

means for receiving both image data corresponding to a captured image of the displayed image and Identification (ID) data associated with an external device utilised to capture the image data; and

means for granting access to the system based on matching the image data received with the generated image and matching the ID data received against the ID data database.

19. The system as claimed in claim 18, wherein the image associated with the current log-in session is, at least in part, randomly generated.

20. The system as claimed in claims 18 or 19, wherein the image comprises:

a first section containing a visual guide for identifying a location of the image in the captured image; and

a second section containing data associated with the current log-in session.

21. The system as claimed in claim 20, wherein the second section associated with the current log-in session is, at least in part, randomly generated.

22. The system as claimed in claim 20, wherein the visual guide comprises a regular geometric shape with a central dot.

23. The system as claimed in claim 22, wherein the regular geometric shape is one of a group consisting of a circle; a triangle; and a square, the dot being concentric with the circle, the triangle, or the square respectively.

24. The system as claimed in any one of claims 18 to 23, wherein the ID data associated with the second device comprises data inherently incorporated in a data communication between the second and first devices.

25. The system as claimed in any one of claims 18 to 24, wherein the ID data comprises comprises one or more of a group consisting of:

Mobile Station ISDN Number (MSISDN);

International Mobile Equipment Identity (IMEI) number;

International Mobile Subscriber Identity (IMSI);

Mobile Identification Number (MIN); and

System Identification Code (SID).

26. The system as claimed in any one of claims 18 to 25, wherein the log-in session comprises a graphical user interface comprising:

a username field for entering user name;

a password field for entering password; and

a area for displaying on the first device the image associated with the current log-in session of the user;

27. The system as claimed in any one of claims 18 to 26, wherein the first device comprises one or more of a group consisting of:

a personal computer; and

an automated teller machine.

28. The system as claimed in any one of claims 18 to 27, wherein the second device comprises one or more of a group consisting of:

a Personal Digital Assistant;

a digital camera; and

a mobile phone.

29. The system as claimed in any one of claims 18 to 28, wherein sending both image data corresponding to the captured image and identification (ID) data associated with the second device from the second device to the first device is through a wireless connection.

30. The system as claimed in any one of claims 18 to 28, wherein sending both image data corresponding to the captured image and the ID data associated with the second device from the second device to the first device is through a wired connection.

31. The system as claimed in any one of claims 18 to 30, wherein both the image data corresponding to the captured image and the ID data are saved by the second device into a memory card, and the first device receives both the image data corresponding to the captured image and the ID data from the memory card.

32. The system as claimed in claim 29, wherein the wireless connection comprises one or more of a group consisting of:

Bluetooth;

infrared;

Wireless LAN;

Ultra-Wideband Radio (UWB); and

HomeRF.

33. The system as claimed in claim 30, wherein the wired connection comprises one or more of a group consisting of:

USB ports and cables;

Firewire ports and cables;

Universal Asynchronous Receiver-Transmitter (UART) based Serial ports and cables; and

parallel ports and cables.

34. The system as claimed in claim 31, wherein the memory card is one of a group consisting of:

MultiMedia Card (MMC);

Secure Digital (SD) cards;

Compact Flash (CF) cards;

Mini Secure Digital card (Mini SD);

Reduced-Size MultiMediaCard (RSMMC);

Memory Stick (MS);

Memory Stick Duo (MS Duo);

Memory Stick Pro (MS Pro);

Memory Stick Duo Pro (MS Duo Pro); and

High Speed Memory Stick (HS MS).

35. A system for user authentication during a log-in session comprising:

an ID data database:

a graphics generator for generating an image associated with a current log-in session of the user;

a screen for displaying the image associated with a current log-in session of the user;

a transceiver for receiving both image data corresponding to a captured image of the displayed image and the ID data associated with an external device utilised to capture the image data; and

an authentication unit for granting access to the system based on matching the image data received with the generated image and matching the ID data received against the ID data database.

Method And System For User Authentication

ABSTRACT

A method and system for user authentication during a log-in session on a first device. The method comprises generating and displaying on the first device an image associated with a current log-in session of the user; capturing the image utilising a second device; sending both image data corresponding to the captured image and Identification (ID) data associated with the second device from the second device to the first device; and granting access to the first device based on matching the image data received with the generated image and matching the ID data received against an ID data database.

Figure 6